REMARKS

Claims 1 – 33 are pending in the application and stand finally rejected. Applicant respectfully requests reconsideration of the pending claims and withdrawal of the final rejection of the claims.

The Examiner rejected claims 1 – 11, 14 – 21, 24 – 28 and 30 – 33 under 35 USC § 103(a) as being unpatentable over *Ballard* (U.S. Patent No. 6,032,137) in view of *Bezy, et al.* (U.S. Pat. No. 5,703,344). The Examiner has newly cited and applied *Bezy, et al.* in finally rejecting these claims. This rejection is respectfully traversed.

The Examiner must satisfy three criteria in order to establish a prima facie case of obviousness: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge of one of ordinary skill in the art, to modify the reference or combine their teachings; (2) there must be a reasonable expectation of success; and (3) the prior art reference or combination of references must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. MPEP §706.02(j), citing *In re Vaeck*, 20 USPQ2d 1438 (Fed. Cir. 1991).

The Examiner stated that *Ballard* does not explicitly teach a real time electronic transaction verification system, but that it would have been obvious to one of ordinary skill at the time the invention was made to modify the *Ballard* invention according to the teachings of *Bezy* because it would provide information from the merchant's point of view if the proper procedures are followed by the merchant to reduce fraud, but nevertheless would be easy and convenient for

the consumer to use, which can be easily implemented in any electronic transaction verification system to obtain a high degree of security.

Applicant incorporates by reference the arguments regarding the teachings of *Ballard* made in the amendment response filed on May 11, 2005. As described therein, *Ballard* teaches a remote image capture system with centralized processing and storage. The image capture system taught by *Ballard* batch processes paper and/or electronic receipts such as credit card receipts, ATM receipts, business expense receipts, and sales receipts, and automatically generates reports such as credit card statements, bank statements, tax reports for tax return preparation, market analyses, etc. (col. 3, ll. 37 – 42, 59 – 64).

The system taught by *Ballard* includes a remote data access subsystem (DATs 200); a data collection subsystem (DACs 400); and a central data processing system (DPC 600). *Ballard* teaches polling and batch processing of data retrieved from data access terminals. DPC 600 polls the DACs 400 to retrieve accumulated data received from the DATs. *Ballard* further teaches, at col. 14, ll. 19 – 33, that the DAC server 402 initiates the polling of DATs and data transmission at optimum poll rate times to decrease the cost of data transmission. As the DAT 200 polling and data transmission progresses, the DAC 400 will periodically update the DPC 600 with its status. The DPC 600 stores the customer's data in a central location, generates reports from the data, and transmits the reports to credit card companies or transaction merchants at remote locations. The DPC 600 has a three tier storage architecture to support the massive storage requirements on the DataTreasury System (col. 16, ll. 27 – 39).

Providing further support that *Ballard* teaches a batch processing systems are the flowcharts of Fig. 3A and Fig. 10. The entire process described in the flowchart of Fig. 3A involves batch processing of scanned paper receipts, i.e., the process occurs after the transactions

have been completed and the paper receipts are available. The flowchart depicted in Fig. 10 for the processing of checks starts by the DataTreasury System capturing the check at the payer's remote location (step 1004) before presenting or mailing the check to the payee. This is for the purpose of comparing the check as written with the check as received by the payee (step 1006) to enable the detection of check alteration. In the paragraph cited by the Examiner (col. 22, ll. 8-17), the check received by the payee in step 1006 is compared with data stored in the DataTreasury System, i.e., the check captured at the payer's remote location. If the check passes this verification (step 1010), an electronic transaction is created (step 1014) and transmitted to the payee bank. If verification fails, an error message is transmitted to the remote location and the system returns to step 1004 for resubmission. An electronic transaction is created only after the check mailed or presented to the payee is verified as being the same as the check originally captured at the payor's location. There is no teaching in *Ballard* of an electronic transaction verification system in which the condition of an authorized user's account is checked in real time. Real time in the context of the invention means responding to transaction, biometric or signature data immediately after the data is entered at the location where the transaction is occurring. Therefore, *Ballard* teaches away from a real time electronic transaction verification system as defined in the claims.

Bezy et al. teaches a system for electronic funds confirmation at the point of transaction. A payor presents a draft to a payee that is confirmed against the account on which it the draft is drawn using a bank identifier and an account identifier electronically read for the draft. The payor bank processor returns a response record indicating whether or not sufficient funds were available. Although *Bezy et al.* returns a confirmation of sufficient funds to the point of transaction in real time, it does not teach a biometric device that selectively transmits biometric

data to a biometric database for comparison with biometric data stored for the authorized user to verify the identity of the individual presenting a transaction token in real time. Thus there is no guarantee that the person presenting a check at a point of transaction is the authorized user/owner of the account.

The Examiner stated that it would have been obvious to combine the teachings of *Ballard* and *Bezy*. However, modifying the *Ballard* system to enable real time electronic transaction verification would add a significant complexity, burden and overhead to the batch processing system. First, neither *Ballard* nor *Bezy, et al.* supports any required suggestion or motivation to make the proposed modification. All the claim limitations must be taught or suggested in the prior art. The Examiner has not cited prior art that teaches all of the claimed limitations of the independent claims. In addition, the complexity of the proposed modification suggests that a person skilled in the art would require significant inventive effort to combine the references as the Examiner suggests. Accordingly, the Examiner has failed to make a prima facie case for obviousness.

Independent claims 1, 14, 24, and 28 include the limitations that the identity of the individual presenting the transaction token and the verification of a condition of a user account are performed in real time, i.e., in order to complete the transaction at the point-of-sale.

With respect to claim 1, *Ballard* fails to teach a transaction information database for storing account information for an authorized user. The Examiner did not cite to *Bezy, et al.* for this feature, and it does not appear that *Bezy, et al.* teaches this feature. In Applicant's invention, an authorized user is an individual authorized to use the electronic transaction verification system. An authorized user can be the account owner, i.e., the person having account information stored in a transaction information database and corresponding biometric data stored

in a biometric database. In *Ballard*, the customer is a vendor or a credit card merchant, not an authorized account user or individual presenting a transaction token at a transaction location. *Ballard* teaches the storing of receipts, not account information for an authorized user. The receipts that are electronically stored are picked up periodically (polled) by the DAC.

Furthermore, *Ballard* fails to teach an electronic transaction verification system for use at a location where a transaction token is presented, in which the reading device selectively transmits transaction information data to the information database for comparison with the account information stored for the authorized user to verify a condition of the account in real time. Although *Ballard* teaches that the DAT could include devices for capturing biometric data for additional security, there is no teaching in *Ballard* or *Bezy et al.* of a biometric data device selectively transmitting biometric data to a biometric database for comparison with biometric data stored for an authorized user to verify the identity of the individual presenting the transaction token in real time. Therefore, claims 1, 14, 24 and 28 are allowable over the combination of *Ballard* and *Bezy, et al.*

Claim 2 – 11 depend directly or indirectly from claim 1; claims 15 – 21 depend directly or indirectly from claim 14; claims 25 – 27 depend directly from claim 24; and claims 30 – 33 depend directly or indirectly from claim 28. Therefore, the dependent claims also are allowable over the combination of *Ballard* and *Bezy, et al.*

Claims 2, 15, 25 and 33 recite the limitation that the transmitted signature data is compared with the signature stored for the authorized user in the signature database in real time. *Ballard* teaches at col. 5, ll. 62 – 63, that DAT scanner 202 is capable of capturing handwritten signatures for identity verification. However, this is not a teaching of verifying the signature of an individual presenting a token in real time. *Bezy et al.* does not teach capturing of an

individual's signature at the point of transaction for identification of the individual. Therefore, claims 2, 15, 25 and 33 are allowable over the combination of *Ballard* and *Bezy, et al.* for this additional reason.

With respect to claims 3 and 16, *Ballard* teaches, at col. 6, ll. 37 – 47, the retrieval of identification information from the card itself for subsequent transmission to the destination of the internet transaction (i.e., the transaction location). Furthermore, the anonymous smart card taught by *Ballard,* at col. 7, lines 7 – 17, does not identify a user at all. The transaction token in Applicant's invention is read in order to transmit transaction information to a transaction information database where the transaction information is compared with stored account information to verify the condition of the user account in real time. The Examiner did not cite to *Bezy, et al.* for this feature, and it does not appear that *Bezy, et al.* teaches this feature. Therefore, claims 3 and 16 are allowable over the combination of *Ballard* and *Bezy, et al.* for this additional reason.

With respect to claims 6 and 18, *Ballard* teaches at col. 5, l. 52 – col. 6, l. 2, that DAT scanner 202 scans a paper receipt and generates a digital bitmap image representation of the receipt. In addition to scanning images and text, the DAT scanner also scans DataGlyph elements. In other words, the scanned paper receipt that is collected from a transaction location by a DAT 200 also scans DataGlyph elements on the receipt. The paper receipt captured by *Ballard* is not a teaching that transaction information data includes data encoded on the transaction token as recited in claims 6 and 18. The Examiner did not cite to *Bezy, et al.* for this feature, and it does not appear that *Bezy, et al.* teaches this feature. Therefore, claims 6 and 18 are allowable over the combination of *Ballard* and *Bezy, et al.* for this additional reason.

With respect to claims 7 and 19, *Ballard* teaches at col. 6, l. 58 – col. 7, l. 3, that the DAT card interface 212 can read transaction data from a smart card that has been lost, stolen, damaged, or deliberately altered in order to reproduce the transaction data for the customer (i.e., merchant). The DAT card interface 212 provides support for independent verification of records maintained by consumers, merchants, and bankers to prevent a loss of data. This is not a teaching of selectively returning a report on customer usages by an electronic transaction verification system as recited in claims 7 and 19. The Examiner did not cite to *Bezy, et al.* for this feature, and it does not appear that *Bezy, et al.* teaches this feature. Therefore, claims 7 and 19 are allowable over the combination of *Ballard* and *Bezy, et al.* for this additional reason.

With respect to claims 8, 20, 26 and 31, *Ballard* teaches, at col. 6, ll. 53 – 58 and col. 7, ll. 41 – 44, that DATs 200 can include additional devices for capturing other biometric data for additional security. These devices include facial scans, fingerprints, voice prints, iris scans, retina scans, and hand geometry. *Ballard* further teaches that DAT controller 210 compresses, encrypts, and tags the bitmap image of a receipt to form a tagged encrypted compressed bitmap image (TECBI). These teachings of *Ballard* do not constitute a teaching of selectively encoding recorded biometric data on the transaction token as recited in claims 8, 20, 26 and 31. In Applicant's invention, a transaction token is presented by an individual at the transaction location. The Examiner did not cite to *Bezy, et al.* for this feature, and it does not appear that *Bezy, et al.* teaches this feature. It is not a paper or electronic receipt generated as a result of the transaction. Therefore, claims 8, 20, 26 and 31 are allowable over the combination of *Ballard* and *Bezy, et al.* for this additional reason.

The Examiner rejected claims 12 – 13, 22 – 23, 29 and 32 under 35 USC § 103(a) as being unpatentable over *Ballard*, in view of *Bezy, et al.*, and further in view of *Hoffman, et. al.*

(U.S. Pat. No. 5,613,012). This rejection is respectfully traversed. Claims 12 – 13, 22 – 23 and 29, 32 depend from claims 1, 14 and 28, respectively. Applicant incorporates by reference the arguments presented above and in Applicant's previous amendment response to distinguish independent claims 1, 14 and 28 from the teachings of *Ballard* and *Bezy, et al.*

In view of the above, it is submitted that the rejections of the Examiner have been properly addressed and the pending claims are in condition for allowance. It is respectfully requested that the Examiner withdrawn his final rejection and allow the pending claims. Such action at an early date is earnestly solicited. It is also requested that the Examiner contact Applicant's attorney at the telephone number listed below should this response not be deemed to place this application in condition for allowance.

Respectfully submitted,

10/6/05
Date

John J. Timar
Registration No. 32,497
Attorney for Applicants

Womble Carlyle Sandridge & Rice, PLLC
P.O. Box 7037
Atlanta, GA 30357-0037
(404) 888-7412 (Telephone)
(404) 870-2405 (Facsimile)